Payment Card Industry (PCI)

Data Security Standard

Summary of Changes from PCI DSS Version 1.1 to 1.2

October 2008

Requirement			
Old	**New**	**Change**	**Type** [i]
General	General	Changed the title of the “PCI DSS Security Audit Procedures” to “PCI DSS Requirements and Security Assessment Procedures” and changed all related references to the document and to the assessment process.	Clarification
General	General	Eliminated stand-alone PCI Data Security Standards document since it is redundant– the “standard” has always been included as the “PCI DSS Requirements’ column in the PCI DSS Security Assessment Procedures document.	Clarification
General	General	Added the table that lists the PCI DSS 6 topics and 12 main requirements, formerly in the PCI Data Security Standard document.	Explanatory
General	General	**PCI DSS Applicability Information** Changed “full magnetic stripe” to “full magnetic stripe data” and added a footnote to define this data.	Clarification
General	General	Clarified “system components’ definition and emphasized use of “system components” term throughout document. In the Scope of Assessment section, clarified the following concepts: network segmentation, scoping, sampling, compensating controls, and third parties/outsourcing. Deleted merchant scoping section and related bullets previously on page 5.	Clarification
General	General	**Instructions and Content for Report on Compliance**: Reordered listed items and enhanced required report content, including detail for scope of review, and clarification for reporting quarterly scanning results.	Clarification Increases quality of report information
General	General	**PCI DSS Compliance - Completion Steps**: Added section to provide guidance on steps to finalize review.	Clarification Mirrors SAQs and PA-DSS
General	General	**Detailed PCI DSS Requirements and Security Assessment Procedures:** Added section title before start of the Report on Compliance template. Included definitions for each of the column headings in the Report on Compliance template.	Clarification
1	1	**Introductory Paragraph:** Added wording to clarify intent of the requirement.	Explanatory
1	1	**General:** Throughout Requirement 1, added routers to clarify that the requirement applies to both firewalls and routers.	Clarification

Requirement		Change	Type [i]
Old	New		
1.1.1	1.1.1	**Requirement & Testing Procedures**: removed "external" to clarify that this requirement applies to all connections to the cardholder data environment.	Clarification
1.1.2	1.1.2	**Testing Procedures**: Added an example of a network diagram "that shows cardholder data flows over the network."	Clarification
1.1.5, 1.1.6 & 1.1.7	1.1.5	**Requirements & Testing Procedures**: Combined 1.1.6 & 1.1.7 into 1.1.5. Former term "risky" changed to "insecure."	Clarification The requirements all covered the same theme.
1.1.8	1.1.6	**Requirement & Testing Procedures:** Renumbered former requirement 1.1.8 to 1.1.6 Changed frequency of rule set review from "quarterly" to "at least every six months." Clarified that documentation should be examined to verify that rule set reviews take place.	Clarification Added flexibility, based on Participating Organization feedback, so controls can be customized to an organization's risk management policies.
1.1.9	N/A	**Deleted Requirement & Testing Procedure**	Clarification Duplicated 1.1
1.2 & 1.3	1.2	**Requirements & Testing Procedures:** Clarified that Requirement 1.2 is to restrict connections between untrusted networks and the cardholder data environment. Combined requirements 1.2 and 1.3 as follows: Requirement 1.2.1 was formerly 1.3.5 and 1.3.7 Requirement 1.2.2 was formerly 1.3.6 Requirement 1.2.3 was formerly 1.3.8 Also made the following clarification: ▪ In 1.2.1.b, added using deny statements as an example for specifically denying traffic not allowed.	Clarification

Requirement		Change	Type [i]
Old	New		
1.3 & 1.4	1.3	**Requirements & Testing Procedures:** Clarified that requirement 1.3 is to restrict direct public access between the Internet and the cardholder data environment. Deleted former Requirement 1.4. Combined Requirements 1.3, and 1.4.as follows: Requirement 1.3.1 was formerly first part of 1.4.1. Requirement 1.3.2 was formerly 1.3.1. Requirement 1.3.3 was formerly latter part of 1.4.1. Requirement 1.3.4 was formerly 1.3.2. Requirement 1.3.5 was formerly 1.4.2. Requirement 1.3.6 was formerly 1.3.3. Requirement 1.3.7 was formerly 1.3.4. Requirement 1.3.8 was formerly 1.5. Also made the following clarifications: ▪ In 1.3.6, replaced “NMAP” with “port scanner” ▪ In 1.3.8, clarified that PAT is an example of NAT	Clarification
1.3.9	1.4	**Requirements & Testing Procedures:** Renumbered from 1.3.9 to 1.4. Split original content of 1.3.9 testing procedure into 1.4.a and 1.4.b.	Clarification Didn’t logically fit into firewall configuration section
2	2	**Introductory Paragraph:** Reworded summary to aid understanding.	Explanatory
2.1.1	2.1.1	**Requirement and Testing Procedure**: Clarified that requirement applies to wireless environments “attached to cardholder environment or transmitting cardholder data.”	Clarification To address scoping/ segmentation FAQ’s
2.1.1	2.1.1	**Requirement & Testing Procedure:** Deleted references to specific wireless technologies like WEP.	Clarification To emphasize using strong encryption technologies for wireless networks, for both authentication and transmission.
2.1.1	2.1.1	**Requirement & Testing Procedure:** Removed requirement to disable broadcast of SSID.	Clarification Disabling SSID broadcast does not prevent a malicious user from determining the SSID, as the SSID is broadcast over numerous other messaging/ communication channels

Requirement		Change	Type [i]
Old	New		
2.1.1	2.1.1	**Requirement & Testing Procedure:** Replaced “access points” with “wireless devices.” Replaced requirement to enable WPA or WPA2 with requirement to update firmware to support strong encryption.	Clarification
2.2	2.2	**Requirement & Testing Procedure:** Moved examples from requirement to testing procedures.	Clarification
2.3	2.3	**Testing Procedure:** Changed bullet for “wireless management interfaces” to “web-based management interfaces.”	Clarification
2.4	2.4	**Requirement & Testing Procedure**: Clarified that this requirement applies to “shared” hosting providers	Clarification
3	3	**Introductory Paragraph:** Expanded first sentence to include examples in addition to encryption (truncation, masking, obfuscation, and hashing).	Explanatory
3.1	3.1	**Testing Procedure:** Simplified third bullet to add clarity.	Clarification
3.2	3.2	**Requirement:** Changed “subsequent to” authorization to “after” authorization.	Clarification
3.2.1	3.2.1	**Requirement:** Removed redundant information from italicized note.	Clarification
3.2.1, 3.2.2. 3.2.3	3.2.1, 3.2.2. 3.2.3	**Testing Procedures:** Removed references to different types of logs, added “All logs,” and provided examples.	Explanatory
3.3	3.3	**Testing Procedures:** Changed the following terms: “specific” need to “legitimate business” need, “credit card data” to “PAN.” Provided examples of where PAN may be displayed.	Clarification
3.4	3.4	**Requirement and Testing Procedures:** Changed “data” to “PAN.” Removed wireless as an example since this requirement applies to all types of platforms. Changed “Strong one-way hash functions (hashed indexes)” to “One-way hashes based on strong cryptography.” Removed references to encryption algorithms and masking. Added “files” to “Examine several tables or files…” Changed “database servers” to “data repositories.“ Removed redundant Procedure 3.4.e.	Clarification

Requirement		Change	Type [i]
Old	New		
3.4.1	3.4.1	**Requirement and Testing Procedures:** Clarified that the example provided should be "local user account databases." Clarified intent of "Verify that decryption keys are not stored on the local system" by changing wording to "Verify that cryptographic keys are stored securely." Provided examples of storing keys securely. Added "cryptographic." Clarified requirement that removable media be encrypted separately.	Clarification
3.5, 3.6	3.5, 3.6	**Requirement:** Changed "encryption" to cryptographic throughout 3.5 and 3.6."	Clarification
3.6	3.6	**Testing Procedures:** Provided example of where Key Management Guidance can be found (NIST).	Explanatory
3.6.1 – 3.6.8	3.6.1 – 3.6.8	**Requirement and Testing Procedures:** Clarified that the testing procedures should include verification that the procedures are implemented.	Clarification
3.6.5, 3.6.8, 3.6.9	3.6.5	**Requirement and Testing Procedures:** Combined Requirements 3.6.8 and 3.6.9 into Requirement 3.6.5.	Clarification
3.6.6	3.6.6	**Requirement and Testing Procedures:** Moved part of requirement included in parentheses to the testing procedures as an example.	Clarification
3.6.10	3.6.8	**Requirement and Testing Procedures:** Re-numbered 3.6.10 to 3.6.8.	N/A
4	4	**Introductory Paragraph:** Reworded summary to aid understanding.	Explanatory
4.1	4.1	**Requirement and Testing Procedure:** Changed former example of "WiFi (IEEE 802.11x)" to "Wireless technologies." Updated SSL to include 'latest patches."	Clarification Addressing SSL 2.0 FAQs
4.1	4.1	**Testing Procedures:** Broke SSL tests into three bullets.	Clarification

Requirement		Change	Type [i]
Old	New		
4.1.1	4.1.1	**Requirement & Testing Procedure:** Clarified that requirement applies to wireless networks transmitting cardholder data "or connected to cardholder data environments." Deleted specific requirements and testing procedures for WEP implementations. Added requirement to implement wireless according to industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. *For new wireless implementations,* it is prohibited to implement WEP after March 31, 2009. *For current wireless implementations*, it is prohibited to use WEP after June 30, 2010.	Enhancement To emphasize using strong encryption technologies for wireless networks, for both authentication and transmission.
4.2	4.2	**Requirement & Testing Procedure:** Changed "e-mail" to "end-user messaging technologies" (e-mail, instant messaging, chat).	Clarification To mirror PA-DSS and address FAQ's.
5	5	**Introductory Paragraph:** Reworded summary to aid understanding.	Explanatory
5.1	5.1	**Requirement & Testing Procedure:** Clarified requirement applies to all operating systems types commonly affected by malicious software, if applicable anti-virus technology exists. Besides use of the term "anti-virus software," changed the term "virus" to "malicious software." Deleted note stating "Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes."	Clarification
5.1.1	5.1.1	**Requirement & Testing Procedure:** Changed "other malicious software" to be "all known types of malicious software." Included viruses, worms, trojans and rootkits as examples of other malicious code that anti-virus software should address.	Clarification
5.2	5.2	**Testing Procedures**: Split former bullets of Testing Procedure 5.2 into separate testing procedures 5.2.a through 5.2.d. Included all operating system types in the sample of system components. Changed "in accordance with company retention policy" to "in accordance with PCI DSS Requirement 10.7."	Clarification & Enhancement Clarified that this log-retention policy should be in line with other log-retention policies required by PCI DSS.

Requirement		Change	Type [i]
Old	New		
6.1	6.1	**Requirements & Testing Procedures**: Noted that an organization can consider prioritizing their process for applying patches. Changed "30 days" to "one month".	Clarification
6.2	6.2	**Requirements**: Clarified that "standards" refers to "configuration standards required by PCI DSS Requirement 2.2".	Clarification
6.3	6.3	**Requirements & Testing Procedures**: Clarified that applications must be developed in accordance with PCI DSS requirements. Separated Testing Procedure 6.3 into 6.3.a and 6.3.b—moved latter half of 6.3 to 6.3.b.	Clarification
6.3.1	6.3.1	**Requirements & Testing Procedures:** Added 6.3.1.1-6.3.1.5 to clarify items to be included in the software development life cycle when testing security patches and software and configuration changes.	Clarification
6.3.7	6.3.7	**Requirements & Testing Procedures**: Added note to detail what type of code this requirement applies to, and that internal parties can perform these code reviews. Updated testing procedure 6.3.7.a to focus on reviews of application code changes for *internal applications*. For 6.3.7.a, added a bulleted list to cover: ▪ That code changes must be reviewed by individuals other than originating code author, and by knowledgeable individuals; ▪ That corrections must be implemented prior to release; ▪ That management must review and approve code review results prior to release. Updated testing procedure 6.3.7.b to focus on reviews of application code changes for *web applications*. For 6.3.7.b, added a bulleted list to cover the above three bullets at 6.3.7.a, plus the following fourth bullet: ▪ That code reviews ensure code is developed according to OWASP & PCI DSS Requirement 6.5.	Clarification
6.4	6.4	**Requirements**: To standardize use of terms, changed "system and software configuration changes" to "changes to system components" and made related change in 6.4.b.	Clarification

Requirement		Change	Type [i]
Old	New		
6.5	6.5	**Requirements & Testing Procedures**: Noted that 1) the current OWASP Guide at the time of the assessment should be used. Added test 6.5.b to verify that developers are knowledgeable about secure coding techniques. Renumbered former test 6.5.b to 6.5.c.	Clarification
6.5.1 – 6.5.10	6.5.1 – 6.5.10	**Requirements & Testing Procedures**: Changed each to match new *Open Web Application Security Project guide* (new "Top Ten").	Clarification
6.6	6.6	**Requirements & Testing Procedures**: Deleted note that this requirement is "a best practice until June 30, 2008" - this is now a requirement. Clarified that this requirement 1) applies to public-facing web applications to address new threats and vulnerabilities on an ongoing basis, 2) that applications can be reviewed with manual or automated application vulnerability assessment tools or methods, and 3) that applications should be reviewed at least annually and for all changes. Replaced "application layer firewall" with "web-application firewall."	Clarification Removed "Best Practice" wording
7	7	**Introductory Paragraph:** Reworded summary to aid understanding.	Explanatory
7.1	7.1	**Requirement & Testing Procedures**: To standardize use of terms, changed "computing resources and cardholder information" to "system components and cardholder data".	Clarification
7.1, 7.2	7.1.1 - 7.1.4, 7.2.1 - 7.2.3	**Requirement & Testing Procedures**: Split bullets of Testing Procedures 7.1 and 7.2 into separate sub-requirements and testing procedures at 7.1.1 through 7.1.4, and 7.2.1 through 7.2.3. Added clarifying text to Testing Procedures.	Clarification
8.1	8.1	**Requirement:** Changed "Identify" to "Assign"	Clarification
8.2	8.2	**Requirement:** Expanded "password" to "password or passphrase". Replaced bullets for "Token devices" and "Biometrics" with "Two-factor authentication" and provided examples for two-factor authentication.	Clarification
8.3	8.3	**Requirement:** Defined "remote access"	Explanatory

Requirement		Change	Type [i]
Old	New		
8.4	8.4	**Requirement & Testing Procedures:** Changed "encrypt all passwords" to "Render all passwords unreadable." Referenced PCI DSS Glossary for definition of strong cryptography. Clarified that the testing procedures should determine if the password is rendered unreadable *in both storage and in transmission.*	Clarification
8.5.1	8.5.1	**Testing Procedures:** Removed 8.5.1.b due to its redundancy.	Clarification
8.5.4	8.5.4	**Testing Procedures:** Changed "inactivated" to "deactivated."	Clarification
8.5.5	8.5.5	**Requirement &Testing Procedure:** Changed "remove" to "remove or disable."	Clarification
8.5.6	8.5.6	**Testing Procedure:** Changed "inactive" to "disabled."	Clarification
8.5.16	8.5.16	**Testing Procedures:** To clarify that access to databases should be restricted to administrators and applications, separated user access, queries, and actions from application access. Changed "SQL" to database.	Clarification
9.1	9.1	**Requirement & Testing Procedure**: Changed "that store, process, or transmit cardholder data" to "in the cardholder data environment".	Clarification
9.1.1	9.1.1	**Requirement & Testing Procedure**: Clarified that "cameras" means "video cameras". Added an alternate option of "other access control mechanisms" in addition to "video cameras" and clarified that the technology must provide ability to monitor "individual physical access". Added note to define "sensitive areas".	Clarification
9.2.a	9.2.a	**Requirement & Testing Procedure**: Removed "contractors" in the testing procedure and added "contractors" as part of the definition of an "employee" in the requirement.	Clarification
9.4	9.4	**Requirement**: Added required contents of visitor logs to align the requirement with the testing procedure.	Clarification
9.5	9.5	**Requirement & Testing Procedure**: To match the testing procedure, added requirement to review the security of the offsite location at least annually, and changed the review cycle from "periodically" to "at least annually" in the testing procedure.	Clarification

Requirement		Change	Type [i]
Old	New		
9.6	9.6	**Requirement & Testing Procedure**: Removed the list of paper and electronic media from the requirement and changed the list in the testing procedure to align with items previously included in the requirement. Clarified "electronic media" in the list as "removable electronic media".	Clarification
9.8	9.8	**Requirement & Testing Procedure**: Clarified "media" as "media that contain cardholder data".	Clarification
9.9	9.9	**Testing Procedure**: Removed "periodic" in the frequency of media inventories. (Defined frequency in 9.9.1.)	Clarification
9.9.1	9.9.1	**Requirement & Testing Procedure**: Clarified that media inventories should be performed at least annually. Removed testing procedure 9.9.1.b.	Clarification Redundant with testing procedure 9.6.
9.10.1	9.10.1	**Requirement & Testing Procedure:** Clarified the destruction of hardcopy materials is such that cardholder data cannot be reconstructed. Removed incorrect ISO standards reference.	Clarification
9.10.2	9.10.2	**Requirement & Testing Procedure**: Clarified that, when electronic media is destroyed, cardholder data must be rendered unrecoverable, which can be achieved via a secure wipe program or by physical destruction.	Clarification
10	10	**Introductory Paragraph:** Reworded summary to aid understanding.	Explanatory
10.1	10.1	**Testing Procedure**: Removed specific reference to wireless networks since requirement applies to all system components.	Clarification
10.2	10.2	**Testing Procedure**: Added to all 10.2 sub requirements wording to ensure events are verified to be "logged."	Clarification
10.3	10.3	**Testing Procedure**: Added to all 10.3 sub requirements wording to ensure these events are verified to "be included in log entries."	Clarification
10.4.a	10.4.a	**Testing Procedure**: Added "a known, stable version" of NTP "kept current per PCI DSS requirements 6.1 and 6.2" to remove redundancy in 10.4.c.	Clarification
10.4.d	10.4.c	**Testing Procedure**: Removed 10.4.c sub-requirement as it was redundant with 10.4.a. Renumbered previous 10.4.d to 10.4.c.	Clarification

Requirement		Change	Type [i]
Old	New		
10.5.4	10.5.4	**Requirement & Testing Procedure**: Changed "copy" to "write" and replaced "wireless networks" with "external facing technologies" and provided "wireless, firewalls, DNS and mail" as examples.	Clarification
10.7	10.7	**Requirement & Testing Procedure**: Replaced "online" reference with "immediately available for analysis" and provided examples (online, archived or restorable from backup).	Clarification To address FAQs and PO feedback on the "online" requirement
11	11	**Introductory Paragraph**: Changed "hackers" to "malicious individuals", and "systems" to "system components". Added language that controls have to adapt to changing environment.	Explanatory
11.1	11.1	**Requirements & Testing Procedures:** Removed general language regarding testing of security controls since this is duplicated by other requirements. Focused requirement on testing for the presence of wireless access points and added option to implement wireless IDS/IPS. Changed 11.1.a to address verification that scanning takes place or that IDS/IPS is implemented. Changed 11.1.b to verify IDS/IPS will generate alerts. Added 11.1.c to ensure Incident Response Plan defines a process to react to unauthorized wireless devices.	Clarification To address duplication of other requirements and provide more flexibility
11.2	11.2	**Requirements & Testing Procedures**: Changed language in note to be consistent with other documentation. Changed 11.2.a to be specific to internal scans and changed "clean" to "passing". Added Note stating ASV is required to perform quarterly external scans, but is not required to perform external scans after network changes or internal scans. Added note to 11.2.b to indicate that for initial assessment only, fewer than 4 quarterly passing scans may be acceptable as long as the most recent scan was a passing scan. Added 11.2.c to verify that scanning is performed after significant network changes, and that scans are repeated until all deficiencies are remediated.	Clarification To address FAQs, clarified that initial compliance is not dependent on four passing scans.
11.3	11.3	**Requirements & Testing Procedures**: Clarified that both external and internal tests must be performed. Created 11.3a for testing procedure previously at 11.3 and added that the testing must be repeated. Added 11.3.b to verify qualifications of individuals performing the tests, and that there is no requirement to use QSA or ASV.	Clarification Qualified internal personnel or external 3rd parties can perform penetration tests.

Requirement		Change	Type [i]
Old	New		
11.3.1	11.3.1	**Testing Procedures**: Added statement indicating test should include components that support network functions as well as operating systems.	Clarification
11.3.2	11.3.2	**Testing Procedures**: Added reference to requirement 6.5 as minimum tests to perform.	Clarification
11.4	11.4	**Requirements & Testing Procedures**: Clarified IDS vs. IPS requirement. Changed monitoring scope from “all network traffic” to “all traffic in the cardholder data environment”. Changed 11.4.a from “Observe the use of”” to “Verify the use of” Changed 11.4b from “is in place to monitor and alert” to “are configured to monitor and alert”.	Clarification
11.5	11.5	**Requirements & Testing Procedures**: Added configuration files. Removed reference to cardholder data files from italicized text. Added examples of types of files to be monitored.	Clarification Cardholder data changes as part of regular business and are not expected to be monitored by file integrity monitoring.
12	12	**Introductory Paragraph**: Provided a definition for “employee” which is applicable for this entire Requirement 12.	Clarification
12.1.1	12.1.1	**Requirement & Testing Procedure**: Changed “requirements in this specification” to “PCI DSS requirements.”	Clarification
12.3	12.3	**Requirement**: Changed list of critical employee-facing technologies to include “remote access technologies, wireless technologies, removable electronic media, e-mail usage, internet usage, laptops, and personal data/digital assistants (PDAs).”	Clarification
12.3.1 and 12.3.2	12.3.1 and 12.3.2	**Testing Procedure**: Changed “devices” to “technologies.”	Clarification
12.3.8 and 12.3.9	12.3.8 and 12.3.9	**Requirement & Testing Procedure**: Changed “modems” to “remote access technologies.”	Clarification
12.3.10	12.3.10	**Requirement & Testing Procedure**: Changed “remotely via modem” to “via remote access technologies.” Generalized media such as floppy disks and external media to “removable electronic media.” Clarified that copy, move and storage functions are prohibited.	Clarification

Requirement		Change	Type [i]
Old	New		
12.6.1	12.6.1	**Requirement & Testing Procedure**: Removed examples in the requirement. Provided more examples in the testing procedure.	Clarification
12.6.2	12.6.2	**Requirement & Testing Procedure**: Clarified that employee acknowledgement must be done at least annually. Provided examples of acknowledgement (in writing or electronically).	Clarification
12.7	12.7	**Requirement & Testing Procedure**: Changed "potential employees" to "potential employees prior to hire."	Clarification Previous confusion around the definition of "potential employees".
12.8	12.8	**Requirement & Testing Procedure**: Changed to focus on policies and procedures to manage service providers, rather than contractual requirements.	Clarification
12.8.1	12.8.1	**Requirement & Testing Procedure**: Replaced with former 12.10.1 but changed the applicability from connected entities to service providers.	Clarification
12.8.2	12.8.2	**Requirement & Testing Procedure**: Changed "contract" to "written agreement." Changed "third party" to "service providers" in the testing procedure.	Clarification
N/A	12.8.3	**Requirement & Testing Procedure**: Formerly 12.10.2 and 12.10.4 but combined as new 12.8.3 and changed the applicability from connected entities to service providers. Clarified that an established process for engaging service providers including proper due diligence is in place prior to engagement.	Clarification
N/A	12.8.4	**Requirement & Testing Procedure**: Formerly 12.10.3 but changed the applicability from connected entities to service providers. Clarified to include a maintenance program to monitor service providers' PCI DSS compliance status.	Clarification Added flexibility, based on Participating Organization feedback so the control can be customized to the organization's risk management policies.
12.9.1	12.9.1	**Requirement & Testing Procedure**: Changed to make the Incident Response Plan contents consistent between the requirement and testing procedure.	Clarification
12.9.3 and 12.9.5	12.9.3 and 12.9.5	**Testing Procedure**: Added "detection of unauthorized wireless devices" in the alerts so that unauthorized wireless devices are not missed	Clarification
12.10	N/A	**Requirement & Testing Procedure**: Deleted (see 12.8 above).	Clarification

Requirement		Change	Type [i]
Old	New		
12.10.1 - 12.10.4	N/A	**Requirement & Testing Procedure**: Deleted (see 12.8.1 - 12.8.4 above).	Clarification
Appendix A	Appendix A	**Shared Hosting Providers:** Clarified that this appendix applies to shared hosting providers.	Clarification
A.1.1	A.1.1	**Requirement:** Clarified that this applies to access via processes run by, or for, a hosted entity.	Clarification
Appendix B	Appendix B	**Compensating Controls:** Clarified compensating controls as needed to mirror clarifications throughout document. Expanded compensating controls explanations and provided examples. Combined previous wording from “Compensating Controls for Requirement 3.4” into main compensating controls explanation.	Clarification
Appendix C	Appendix C	**Compensating Controls Worksheet:** Clarified compensating controls as needed to mirror clarifications throughout document.	Clarification
N/A	Appendix D	**Attestation of Compliance for Onsite Assessments – Merchants**: Added standard attestation of compliance forms to be completed and signed by merchants and/or QSAs.	Enhancement
N/A	Appendix E	**Attestation of Compliance for Onsite Assessments – Service Providers**: Added standard attestation of compliance forms to be completed and signed by service providers and QSAs.	Enhancement
N/A	Appendix F	**PCI DSS Reviews – Scoping and Sampling**: Added flowchart to depict scoping and sampling processes, to be used by assessors conducting PCI DSS reviews.	Clarification

[i]

Explanatory:	Explanations and/or definitions to increase understanding
Clarification:	Clarifies intent of requirement
Enhancements:	Changes needed to ensure ongoing integrity so that the standard continues to adequately address risks